Name : Vaibhav Soni

Enrolment No. : IU2141230287

Branch : CSE – A

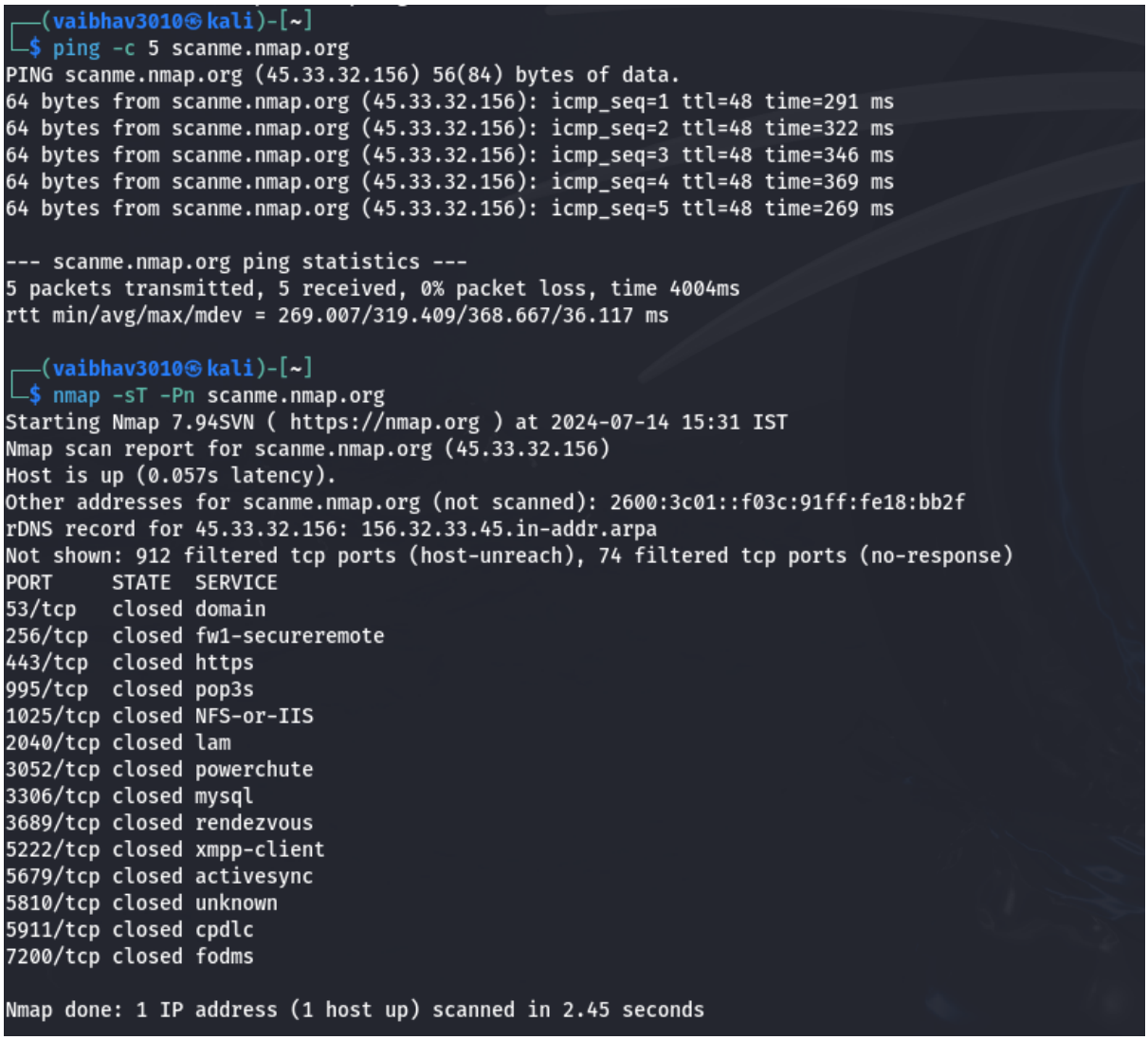
Sem : 7

Subject : Cyber Security

Lab – 1

Aim : TCP Scanning using NMAP.

Output :



```
┌──(vaibhav3010㉿kali)-[~]
└─$ ping -c 5 scanme.nmap.org
PING scanme.nmap.org (45.33.32.156) 56(84) bytes of data.
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=1 ttl=48 time=291 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=2 ttl=48 time=322 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=3 ttl=48 time=346 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=4 ttl=48 time=369 ms
64 bytes from scanme.nmap.org (45.33.32.156): icmp_seq=5 ttl=48 time=269 ms

--- scanme.nmap.org ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 269.007/319.409/368.667/36.117 ms

┌──(vaibhav3010㉿kali)-[~]
└─$ nmap -sT -Pn scanme.nmap.org
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-14 15:31 IST
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.057s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
rDNS record for 45.33.32.156: 156.32.33.45.in-addr.arpa
Not shown: 912 filtered tcp ports (host-unreach), 74 filtered tcp ports (no-response)
PORT     STATE  SERVICE
53/tcp   closed domain
256/tcp  closed fw1-secureremote
443/tcp  closed https
995/tcp  closed pop3s
1025/tcp closed NFS-or-IIS
2040/tcp closed lam
3052/tcp closed powerchute
3306/tcp closed mysql
3689/tcp closed rendezvous
5222/tcp closed xmpp-client
5679/tcp closed activesync
5810/tcp closed unknown
5911/tcp closed cpdlc
7200/tcp closed fodms

Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds
```

Conclusion :

- The `ping` command executed on `scanme.nmap.org` shows successful connectivity, with 5 packets transmitted and received, and no packet loss. The round-trip times range from 269 ms to 369 ms, indicating a stable connection with a consistent response time. This confirms that the host is reachable over the network, despite some latency.

- The `nmap` scan using the `-sT -Pn` options reveals that `scanme.nmap.org` is up but has all scanned ports closed. The scan checked numerous ports, such as 53 (domain), 443 (https), and 3306 (mysql), and found them all closed. Additionally, it reported that 912 filtered ports were not reachable, suggesting that firewall or filtering rules are in place, preventing access to these ports. This indicates a highly secured network configuration on the target host.